I. HIPAA and Research at Brown

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations, including the Privacy Rule and the Security Rule, as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act, govern the way certain health information is collected, maintained, used, and disclosed. The Privacy Rule establishes a set of safeguards around certain types of health information known as Protected Health Information (PHI) and sets forth a national minimum level of protection for PHI. It also describes ways in which a Covered Entity can use or disclose PHI for research purposes.

B. Brown University is not a Covered Entity under HIPAA for the purpose of research. As a Brown researcher, you may wish to receive PHI from a Covered Entity and therefore must understand your obligations to ensure that data are released to you in a manner that complies with HIPAA and that you appropriately protect those data at Brown once received.

II. Disclosure of PHI to Brown for Research Purposes

A. There are circumstances in which health information maintained by a covered entity is not protected by the Privacy Rule. PHI excludes health information that is de-identified. Health information that is de-identified can be used and disclosed by a covered entity without Authorization or any other permission specified in the Privacy Rule. Under the Privacy Rule, covered entities may determine that health information is not individually identifiable in either of two ways as described below.

B. The Privacy Rule permits covered entities to use and disclose PHI without Authorization for certain types of research activities. For example, PHI can be used or disclosed for research if the covered entity obtains documentation that its Institutional Review Board (IRB) or Privacy Board has waived the requirement for Authorization or allowed an alteration to Authorization.

C. The Privacy Rule allows a covered entity to enter into a Data Use Agreement for sharing a limited data set.

D. There are provisions for how PHI can be used or disclosed for activities preparatory to research and for research on decedents' information.

E. Please be aware that (with some exceptions) the Privacy Rule imposes a minimum necessary requirement on all permitted uses and disclosures of PHI by a covered entity. This means that a covered entity must apply policies and procedures, or criteria it has developed, to limit certain uses or disclosures of PHI, including those for research purposes, to "the information reasonably necessary to accomplish the purpose [of the sought or requested use or
"As with all human subjects research activities, it's prudent to only ask for the data you need to accomplish your research objectives.

III. Business Associate Agreements

It is rare that any Brown researcher is truly acting in the capacity of a Business Associate in the conduct of his/her research at Brown; researchers are not business associates solely by virtue of their own research activities (although one may become a business associate in some other capacity, e.g., if you are de-identifying PHI on behalf of a covered entity). You may find that covered entities that are inexperienced with providing PHI to research institutions insist that entering into a Business Associate Agreement is the only way to provide PHI to Brown. This is not the case. Brown is able to appropriately protect these sensitive data without engaging in a Business Associate Agreement by using Stronghold for data storage.

IV. De-Identification of PHI under the Privacy Rule

De-identified data are not subject to the requirements of the Privacy Rule because they are not individually identifiable. There are two ways to de-identify data:

1. The Safe Harbor Method: provides that all of the following elements are removed from a data set:
   - Name
   - All geographic subdivisions smaller than a state (street address, city, county, precinct)
   - Note: zip code or equivalents must be removed, but can retain first 3 digits of the geographic unit to which the zip code applies if the zip code area contains more than 20,000 people
   - For dates directly related to individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death)
   - All ages over 89 or dates indicating such an age
   - Telephone number
   - Fax number
   - Email address
   - Social security number
   - Medical record number
   - Health plan number
   - Account numbers
   - Certificate or license numbers
   - Vehicle identification/serial numbers, including license plate numbers
   - Device identification/serial numbers
   - Universal Resource Locators (URLs)
   - Internet Protocol (IP) addresses
   - Biometric identifiers, including finger and voice prints
   - Full face photographs and comparable images
   - Any other unique identifying number, characteristic, or code. (This effectively a “catch-all” provision and is intended to include items that are not otherwise specified but could make a data set identifiable.)

2. Statistical Method: using the Statistical Method, certification is provided by “a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable so that there is a ‘very small’ risk that the information could be used by the recipient to identify the individual.
who is the subject of the information, alone or in combination with other reasonably available information.”

V. Waiver of Alteration of Authorization

A. In many situations, research cannot be conducted using health information that has been de-identified and it may not be feasible to obtain a signed Authorization for all PHI needed for the conduct of your research. Therefore, the Privacy Rule contains criteria for waiver or alterations of Authorizations by an IRB or another review body called a "Privacy Board."

B. For disclosure of PHI for research purposes, an IRB or Privacy Board may approve a waiver or an alteration of the Authorization requirement in whole or in part. A complete waiver occurs when the IRB or Privacy Board determines that no Authorization will be required for a covered entity to use and disclose PHI for a particular research project. A partial waiver of Authorization occurs when an IRB or Privacy Board determines that a covered entity does not need Authorization for all PHI uses and disclosures for research purposes, such as disclosing PHI for research recruitment purposes. An IRB or Privacy Board may also approve a request that removes some PHI, but not all, or alters the requirements for an Authorization (an "alteration").

C. Documentation of the waiver or alteration of Authorization must include a statement identifying the IRB or Privacy Board that made the approval and the date of approval. Among other things, the documentation must also include statements that the IRB or Privacy Board has determined that the waiver or alteration of Authorization, in whole or in part, satisfies the following criteria:

1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
   a. An adequate plan to protect health information identifiers from improper use and disclosure.
   b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so).
   c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule.

2. The research could not practicably be conducted without the waiver or alteration.

3. The research could not practicably be conducted without access to and use of the PHI.

D. Many research projects take place at multiple sites and/or require the use and disclosure of PHI created or maintained by more than one covered entity. The Privacy Rule does not require approval of a waiver or an alteration of Authorization by more than one IRB or Privacy Board; a covered entity may rely on a waiver or an alteration of Authorization approved by any IRB or Privacy Board, without regard to the location of the approver.

VI. Receiving a Limited Data Set with a Data Use Agreement

A. A covered entity may also provide PHI to you in the form of a limited data set for the purpose of research without obtaining an Authorization or documentation of a waiver or alteration of Authorization when the release of data is accompanied by a Data Use Agreement.
B. A Limited Data Set is PHI that excludes the below 16 categories of direct identifiers, but may include: city, state, ZIP code, elements of date, and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed below apply both to information about the individual and to information about the individual's relatives, employers, or household members.

- Names
- Postal address information, other than town or city, state, and ZIP Code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images

C. A Data Use Agreement is a formal, written agreement into which the covered entity enters with Brown/the researcher and establishes specific ways in which the data may be used and how it must be protected. At Brown, Data Use Agreements must be reviewed and signed by the Industry Engagement and Commercial Venturing Office. The School of Public Health leadership has authorization to review and sign its own Data Use Agreements. Whenever you enter into a Data Use Agreement for receipt of a limited data set for human subject research at Brown, you must include a copy of your Data Use Agreement with your protocol submission to the Brown IRB. Brown's Stronghold Research Environment for Data Compliance is available to all Brown researchers for secure computing and storage, and is the recommended environment for use and storage of sensitive data that are subject to a Data Use Agreement.

VII. Activities Preparatory to Research

For activities involved in preparing for research, covered entities may use or disclose PHI to a Brown researcher without an individual's Authorization, a waiver or an alteration of Authorization, or a Data Use Agreement. Instead, the covered entity must obtain from the Brown researcher representations that (1) the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; (2) the PHI will not be removed from the covered entity in the course of review; and (3) the PHI for which use or access is requested is necessary for the research. The covered entity may permit the researcher to make these representations in written or oral form.

Brown researchers should note that any preparatory research activities involving human subjects research which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy informed consent requirements.

VIII. Research on Decedents' Protected Health Information

To use or disclose PHI of the deceased for research, covered entities are not required to obtain
Authorizations from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a Data Use Agreement. Instead, the covered entity must obtain from the Brown researcher who is seeking access to decedents' PHI (1) oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents; (2) oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes; and (3) documentation, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researcher.